MATH 546, HOMEWORK SOLUTIONS, SPRING 2023

(1) Recall the group $S_n = \mathrm{Sym}(\{1,...,n\})$, where S_n is the set of invertible functions from $\{1,\dots,n\}$ to $\{1,\dots,n\}$. The operation in S_n is function composition.

(a) Take $n = 3$. Let σ and τ be the following elements of S_3:

$$\sigma(1) = 2, \quad \sigma(2) = 1, \quad \sigma(3) = 3, \quad \text{and}$$
$$\tau(1) = 2, \quad \tau(2) = 3, \quad \tau(3) = 1.$$

(i) How many distinct elements[1] of S_3 can be written in the form $\sigma^i \circ \tau^j$?

Answer: We see that $\sigma^2 = \mathrm{id}$, $\tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, and $\tau^3 = \mathrm{id}$. Thus, there are **at most** six elements of S_3 of the form $\sigma^i \circ \tau^j$ because we may always insist that $i \in \{0,1\}$ and $j \in \{0,1,2\}$. We have not yet demonstrated that these six functions are distinct. But they in fact are:

i	j	$\sigma^i \circ \tau^j$
0	0	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
0	1	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
0	2	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
1	0	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
1	1	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
1	2	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

We see that there are six different functions of the form $\sigma^i\tau^j$. The group S_3 only has six elements; thus every element of S_3 can be written in the form $\sigma^i\tau^j$.

[1] If f is an element of S_3, then one relatively convenient way to record f is in the form

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

If one uses this notation, then

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

(ii) Can $\tau \circ \sigma$ be written in the form $\sigma^i \circ \tau^j$?

Answer: We saw already that the answer is yes. We can also compute

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma \circ \tau^2.$$

(iii) Record the multiplication table for the smallest subgroup of S_3 which contains τ and σ. Put your entries in the form $\sigma^i \circ \tau^j$ whenever this makes sense.

Answer: Here is the multiplication table for S_3.

	id	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
id	id	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
τ	τ	τ^2	id	$\sigma\tau^2$	σ	$\sigma\tau$
τ^2	τ^2	id	τ	$\sigma\tau$	$\sigma\tau^2$	σ
σ	σ	$\sigma\tau$	$\sigma\tau^2$	id	τ	τ^2
$\sigma\tau$	$\sigma\tau$	$\sigma\tau^2$	σ	τ^2	id	τ
$\sigma\tau^2$	$\sigma\tau^2$	σ	$\sigma\tau$	τ	τ^2	id

Apparently I have started to write $\sigma\tau$ to mean $\sigma \circ \tau$
Notice that the multiplication table for S_3 is the same as the multiplication table for D_3 in problem 10. (Each ρ from problem 10 is written as τ in the present problem.)

(b) Take $n = 4$. Let σ and τ be the following elements[2] of S_4:

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 1, \quad \sigma(4) = 4, \quad \text{and}$$

$$\tau(1) = 2, \quad \tau(2) = 3, \quad \tau(3) = 4, \quad \tau(4) = 1.$$

(i) How many distinct elements of S_4 can be written in the form $\sigma^i \circ \tau^j$?

Answer: We see that $\sigma^2 = \text{id}$, $\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $\tau^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, and $\tau^4 = \text{id}$. Thus, there are **at most** eight elements of S_4 of the form $\sigma^i \circ \tau^j$ because we may always insist that $i \in \{0,1\}$ and $j \in \{0,1,2,3\}$. We have not yet demonstrated

[2] In the notation of footnote 1,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

that these eight functions are distinct. But they in fact are:

i	j	$\sigma^i \circ \tau^j$
0	0	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$
0	1	$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$
0	2	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$
0	3	$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$
1	0	$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$
1	1	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$
1	2	$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$
1	3	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

.

We see that there are eight different functions of the form $\sigma^i\tau^j$.

(ii) Can $\tau \circ \sigma$ be written in the form $\sigma^i \circ \tau^j$?

Answer: We compute $\tau \circ \sigma = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = \sigma \circ \tau^3$.

(iii) Record the multiplication table for the smallest subgroup of S_4 which contains τ and σ. Put your entries in the form $\sigma^i \circ \tau^j$ whenever this makes sense.

Answer: Let G be the smallest subgroup of S_4 which contains τ and σ. We learned in (i) and (ii) that G consists of the eight distinct functions $\sigma^i\tau^j$, where $i \in \{0,1\}$ and $j \in \{0,1,2,3\}$. It is now easy to calculate that the multiplication table for G is

	id	τ	τ^2	τ^3	σ	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$
id	id	τ	τ^2	τ^3	σ	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$
τ	τ	τ^2	τ^3	id	$\sigma\tau^3$	σ	$\sigma\tau$	$\sigma\tau^2$
τ^2	τ^2	τ^3	id	τ	$\sigma\tau^2$	$\sigma\tau^3$	σ	$\sigma\tau$
τ^3	τ^3	id	τ	τ^2	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$	σ
σ	σ	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$	id	τ	τ^2	τ^3
$\sigma\tau$	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$	σ	τ^3	id	τ	τ^2
$\sigma\tau^2$	$\sigma\tau^2$	$\sigma\tau^3$	σ	$\sigma\tau$	τ^2	τ^3	id	τ
$\sigma\tau^3$	$\sigma\tau^3$	σ	$\sigma\tau$	$\sigma\tau^2$	τ	τ^2	τ^3	id

Notice that the multiplication table for this problem is the same as the multiplication table for D_4 in Example (11f) from page 9 of the Lecture

Notes. (Each ρ from the Lecture Notes is written as τ in the present problem.)

(c) Take $n = 4$. Let σ and τ be the following elements of S_4:

$$\sigma(1) = 2, \quad \sigma(2) = 1, \quad \sigma(3) = 3, \quad \sigma(4) = 4, \quad \text{and}$$
$$\tau(1) = 2, \quad \tau(2) = 3, \quad \tau(3) = 4, \quad \tau(4) = 1.$$

(i) How many distinct elements of S_4 can be written in the form $\sigma^i \circ \tau^j$?

Answer: Again 8.

(ii) Can $\tau \circ \sigma$ be written in the form $\sigma^i \circ \tau^j$?

Answer: No.

(iii) Prove that the smallest subgroup of S_4 which contains τ and σ is all of S_4.

Let H be the smallest subgroup of S_4 which contains $\sigma = (12)$ and $\tau = (1234)$. We show that all six transpositions (ij) are in H.
Every element of S_4 is a product of transpositions.
Keep in mind that $(1234)^{-1} = (1432)$.
Observe that

$$(1432)(12)(1234) = (14) \in H,$$
$$(1432)(14)(1234) = (34) \in H,$$
$$(1432)(34)(1234) = (23) \in H,$$
$$(14)(12)(14) = (24) \in H, \text{ and}$$
$$(23)(12)(23) = (13) \in H.$$

The proof is complete.

(2) Consider the following sets S with binary operation $*$. Which pairs $(S, *)$ form a group? If $(S, *)$ is not a group, which axioms fail?

(a) Let S be the set of integers $\mathbb{Z}$ and let $a * b = ab$.

Answer: No $(S, *)$ is not a group. The identity element of S is 1. However, the only elements of S with an inverse are 1 and -1.

(b) Let S be the set of integers $\mathbb{Z}$ and let $a * b = \max\{a, b\}$.

Answer: No $(S, *)$ is not a group. There is no identity element. (If one thinks that a_0 is an identity element of S, then $a_0 - 1 \in S$, but $(a_0 - 1) * a_0 = a_0$. Hence $b * a_0$ is not equal to b for all b in S.)
Of course, then S also does not have inverses.

(c) Let S be the set of integers $\mathbb{Z}$ and let $a * b = a - b$.

Answer: No $(S, *)$ is not a group. The operation $*$ does not associate. Indeed,

$$(1 * 2) * 3 = (1 - 2) - 3 = -4 \text{ but } 1 * (2 * 3) = 1 - (2 - 3) = 1 + 1 = 2.$$

(d) Let S be the set of integers $\mathbb{Z}$ and $a*b=|ab|$.

Answer: No $(S,*)$ is not a group. There is no identity element. (If one thinks that a_0 is an identity element of S, then $1=a_0*1=|a_0|$ and $-1=a_0*(-1)=|-a_0|=|a_0|$; thus, $1=-1$. Of course, that makes no sense.

Also S does not have inverses.

(e) Let S be the set of positive real numbers $\mathbb{R}^+$ and $a*b=ab$.

Answer: Yes, $(S,*)$ is a group.

(f) Let S be the set of non-zero rational numbers $\mathbb{Q}\setminus\{0\}$ and $a*b=ab$.

Answer: Yes, $(S,*)$ is a group.

(3) Prove that multiplication of 2×2 matrices satisfies the associative law.

Answer: Let

$$A=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix},\quad B=\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix},\quad\text{and}\quad C=\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}.$$

We compute

$$\begin{aligned}A(BC)&=A\left(\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}\right)\\&=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\begin{bmatrix}b_{11}c_{11}+b_{12}c_{21}&b_{11}c_{12}+b_{12}c_{22}\\b_{21}c_{11}+b_{22}c_{21}&b_{21}c_{12}+b_{22}c_{22}\end{bmatrix}\\&=\begin{bmatrix}a_{11}(b_{11}c_{11}+b_{12}c_{21})+a_{12}(b_{21}c_{11}+b_{22}c_{21})&a_{11}(b_{11}c_{12}+b_{12}c_{22})+a_{12}(b_{21}c_{12}+b_{22}c_{22})\\a_{21}(b_{11}c_{11}+b_{12}c_{21})+a_{22}(b_{21}c_{11}+b_{22}c_{21})&a_{21}(b_{11}c_{12}+b_{12}c_{22})+a_{22}(b_{21}c_{12}+b_{22}c_{22})\end{bmatrix}\end{aligned}$$

and

$$\begin{aligned}(AB)C&=\left(\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\right)C\\&=\begin{bmatrix}a_{11}b_{11}+a_{12}b_{21}&a_{11}b_{12}+a_{12}b_{22}\\a_{21}b_{11}+a_{22}b_{21}&a_{21}b_{12}+a_{22}b_{22}\end{bmatrix}\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}\\&=\begin{bmatrix}(a_{11}b_{11}+a_{12}b_{21})c_{11}+(a_{11}b_{12}+a_{12}b_{22})c_{21}&(a_{11}b_{11}+a_{12}b_{21})c_{12}+(a_{11}b_{12}+a_{12}b_{22})c_{22}\\(a_{21}b_{11}+a_{22}b_{21})c_{11}+(a_{21}b_{12}+a_{22}b_{22})c_{21}&(a_{21}b_{11}+a_{22}b_{21})c_{12}+(a_{21}b_{12}+a_{22}b_{22})c_{22}\end{bmatrix}\end{aligned}$$

Observe that $A(BC)=(AB)C$.

(4) Is the group $\mathrm{GL}_n(\mathbb{R})$ an Abelian group? Give a proof or counterexample. Recall that $\mathrm{GL}_n(\mathbb{R})$ is the group of invertible $n\times n$ matrices under multiplication.

Answer: No $\mathrm{GL}_n(\mathbb{R})$ is not an Abelian group for $n\geq 2$. In particular, if

$$A=\left[\begin{array}{cc|c}1&1&Z_{1\times(n-2)}\\0&1&Z_{1\times(n-2)}\\\hline Z_{(n-2)\times 1}&Z_{(n-2)\times 1}&I_{n-2}\end{array}\right]\quad\text{and}\quad B=\left[\begin{array}{cc|c}1&0&Z_{1\times(n-2)}\\1&1&Z_{1\times(n-2)}\\\hline Z_{(n-2)\times 1}&Z_{(n-2)\times 1}&I_{n-2}\end{array}\right],$$

then

$$AB=\left[\begin{array}{cc|c}2&1&Z_{1\times(n-2)}\\1&1&Z_{1\times(n-2)}\\\hline Z_{(n-2)\times 1}&Z_{(n-2)\times 1}&I_{n-2}\end{array}\right]\text{ and }BA=\left[\begin{array}{cc|c}1&1&Z_{1\times(n-2)}\\1&2&Z_{1\times(n-2)}\\\hline Z_{(n-2)\times 1}&Z_{(n-2)\times 1}&I_{n-2}\end{array}\right],$$

where $Z_{p\times q}$ is $p\times q$ matrix of zeros and I_{n-2} is the $(n-2)\times(n-2)$ identity matrix. Observe that $AB\neq BA$ and A and B both are invertible matrices.

(5) Write a multiplication table for the following set of matrices over $\mathbb{Q}$:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Answer:

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Notice that this $\{I,A,B,C\}$ is a subgroup[3] of $\mathrm{GL}_2(\mathbb{Q})$ because the multiplication table shows that $\{I,A,B,C\}$ is closed under matrix multiplication and that the inverse of every element of $\{I,A,B,C\}$ is actually in $\{I,A,B,C\}$.

The group $\{I,A,B,C\}$ is easy to recognize. The group has four elements. Every element squares to the identity and the product of any two non-identity elements is the third non-identity element. Every group of this form is called a Klein four group. "Another"[4] Klein four group appears in the class lectures at the end of Example 11 on the bottom of page 9.

(6) Let $G = \{x \in \mathbb{R} \mid 0 < x \text{ and } x \neq 1\}$. Define $a * b = a^{\ln b}$, for a and b in G. Prove that $(G,*)$ is an Abelian group.

Answer:

• We first show that $(G,*)$ is closed. Take a and b in G. We must show that $a*b$ is in G. That is, we must show that $a^{\ln b}$ is a positive real number which is not equal to 1. The real number a is positive, so $a^{\ln b}$ is a real number. The real number a is positive, so $a = e^{\ln a}$ and $a^{\ln b} = e^{\ln a \ln b}$. The graph of $y = e^x$ is ABOVE the x-axis for all x. Thus $a^{\ln b}$ is a positive real number. We prove that $a^{\ln b} \neq 1$ by contradiction. If $a^{\ln b} = 1$, then take ln of both sides to learn that $\ln b \ln a = \ln 1 = 0$; hence $\ln b = 0$ or $\ln a = 0$; that is $b = 1$ or $a = 1$. But a and b are both in G; so neither is 1. This is a contradiction. We conclude that $a^{\ln b} \neq 1$. We have shown that if a and b are in G, then $a*b$ is in G.

• We already saw that $*$ commutes. Indeed, if $a,b \in G$, then

$$a*b = a^{\ln b} = e^{\ln a \ln b} = e^{\ln b \ln a} = b^{\ln a} = b*a.$$

[3]Recall that if H is a subset of the group $(G,*)$ and H is a group with the same operation $*$ as G, then H is a subgroup of G. To test that a (non-empty) subset H of G is a subgroup it suffices to verify that H is closed and that the inverse of every element of H in G is actually an element of H. Indeed, the operation $*$ associates on all of G, so it associates on the subset H. Also, the closure properties of H ensure that the identity element of G is actually in H.

[4]I put quotation marks around the word another because the groups are exactly the same. The one on this page is the matrix representation of the one in the class notes.

• The real number e is the identity element of G. Indeed,

$$a * e = a^{\ln e} = a^1 = a$$

for all a in G. We already saw that $e * a = a * e$.

• If $a \in G$, then the inverse of a is $e^{\frac{1}{\ln a}}$. First we observe that $e^{\frac{1}{\ln a}}$ is indeed an element of G. Well, a is positive and not 1; so $\ln a$ is a real number which is not zero. Thus, $\frac{1}{\ln a}$ is a real number which is not zero and $e^{\frac{1}{\ln a}}$ is a positive real number which is not 1. Now we calculate

$$a * e^{\left(\frac{1}{\ln a}\right)} = a^{\ln\left(e^{\left(\frac{1}{\ln a}\right)}\right)} = a^{\frac{1}{\ln a}} = e^{\ln a \frac{1}{\ln a}} = e^1 = e.$$

We already saw that $*$ commutes so we need no check that $e^{\frac{1}{\ln a}} * a = e$.

• We show that $*$ associates. Take a, b, c in G. Observe that

$$a * (b * c) = a * (b^{\ln c}) = a * (e^{(\ln b \ln c)}) = a^{\ln\left(e^{(\ln b \ln c)}\right)} = a^{(\ln b \ln c)}$$
$$= e^{\ln a (\ln b \ln c)} = e^{(\ln a \ln b) \ln c} = (a * b)^{\ln c} = (a * b) * c.$$

Remark. In Homework problem 83 you will prove that the group $(G, *)$ is a disguised version of a very familiar group!

(7) Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ by $a * b = a + b + ab$, for a and b in S. Prove that $(S, *)$ is a group.

Answer:

• We first show that $(S, *)$ is closed. Take a and b in S. It is clear that $a * b$ is a real number. We must show that $a * b = -1$. We argue by contradiction. If $a * b = -1$, then $a + b + ab = -1$; so $ab + a + b + 1 = 0$. In other words, $(a + 1)(b + 1) = 0$ and $a = -1$ or $b = -1$. Neither of these outcomes is possible. Thus $a * b \neq -1$ and $a * b$ is indeed in S.

• We notice that $*$ commutes!

• Observe that 0 is the identity element of $(S, *)$ because

$$a * 0 = a + 0 + a(0) = a.$$

We need not check that $0 * a = a$ because we already observed that $a * b = b * a$ for all a and b in S.

• We observe that $*$ associates. Indeed, if a, b, c are in S, then

$$a * (b * c) = a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = (a + b + ab) + c + (a + b + ab)c$$
$$= a * b + c + (a * b)c = (a * b) * c.$$

• Let a be an element of S. We observe that the inverse of a is $\frac{-a}{a+1}$. First of all, we notice that the proposed inverse is a Real number because $a \neq -1$.

We also notice that $\frac{-a}{a+1} \neq -1$ because $0 \neq -1$. Thus, the proposed inverse is an actual element of $(S,*)$. Finally, we verify that

$$a * \left(\frac{-a}{a+1}\right) = a + \left(\frac{-a}{a+1}\right) + a\left(\frac{-a}{a+1}\right) = \frac{a(a+1)-a-a^2}{a+1} = \frac{0}{a+1} = 0.$$

Remark. In Homework problem 78 you will prove that the group $(S,*)$ is a disguised version of a very familiar group!

(8) Prove that a non-Abelian group must have at least five distinct elements.

Answer:

• Let G be a group.

• Notice that the identity element commutes with every element of G.

• Notice that if a is an element of G, then a commutes with a and a commutes with the inverse of a.

• Notice that if a and b are elements of G which do not commute, then $ab \neq \text{id}$.

(Indeed, if $ab = \text{id}$, then multiply both sides of the equation on the left by the inverse of a to see that b is equal to the inverse of a. However, a and the inverse of a commute but a and b do not commute.)

• Notice that if a and b are elements of G which do not commute, then $ab \neq a$.

(Indeed, if $ab = a$, then multiply both sides of the equation on the left by the inverse of a to see that $b = \text{id}$. However a and id do commute, but a and b do not commute.)

• Notice that if a and b are elements of G which do not commute, then $ab \neq b$.

(Indeed, if $ab = b$, then multiply both sides of the equation on the right by the inverse of b to see that $a = \text{id}$. However b and id do commute, but b and a do not commute.)

• Now we are ready to write the proof. If a and b are elements of the group G with $ab \neq ba$, then a, b, ab, ba, and id are FIVE different elements of G.

(9) Let G be a group and let a, b be elements of G. Suppose $(ab)^2 = a^2b^2$. Prove that a and b commute.

Answer: We are given

$$abab = aabb.$$

Multiply both sides of the equation on the left by the inverse of a and multiply both sides of the equation on the right by the inverse of b to obtain $ba = ab$.

(10) Is the group of complex numbers $\{1,-1,i,-i\}$, under multiplication, a Klein 4-group?

Answer: The above group (which we usually call U_4) is NOT a Klein four group. In a Klein 4 group every element squares to the identity element. The identity element of U_4 is 1. The elements i and $-i$ both square to -1, which is not the identity element.

The group U_4 is a cyclic group generated by either i or $-i$.

(11) Let ρ be rotation counterclockwise by 120° fixing the origin. Let σ be reflection of the xy plane across the x axis. Let D_3 be the smallest subgroup of the group of rigid motions which contains ρ and σ.
   (a) List the elements of D_3.
   (b) Find the multiplication table for D_3.
   (c) Describe the action of each element of D_3.
   (d) Show that if $\tau \in D_3$, then $\tau(T) = T$, where T is the triangle with vertices $(1,0)$, $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$, and $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$.

Answer: Notice that T is the equilateral triangle (each side has length $\sqrt{3}$) with vertices

$$\begin{aligned} P &= e^0 = 1, \\ Q &= e^{\frac{2\pi i}{3}} = \cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3} = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}, \text{ and} \\ R &= e^{\frac{4\pi i}{3}} = \cos\tfrac{4\pi}{3} + i\sin\tfrac{4\pi}{3} = -\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}. \end{aligned}$$

Observe that

$$\begin{aligned} &\rho(P) = Q, && \rho(Q) = R, && \rho(R) = P \\ &\sigma(P) = P, && \sigma(Q) = R, && \sigma(R) = Q \\ &\sigma\rho(P) = \sigma(Q) = R, && \sigma\rho(Q) = \sigma(R) = Q, \text{ and} && \sigma\rho(R) = \sigma(P) = P \end{aligned}$$

So $\sigma\rho$ is reflection across the line connecting the origin and Q. (If that discussion is not sufficiently convincing to you then recall that that rotation counterclockwise by θ is the linear transformation $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$ and reflection of the xy-plane across the line through the origin with angle θ is the linear transformation $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$. Use these formulas and various Trig identities to verify the claims.)

Once we are confident that $\sigma\rho$ is a reflection, then we know that

$$(\sigma\rho)(\sigma\rho) = \mathrm{id}\,.$$

Multiply both sides on the the left by σ (which is the inverse of σ) and on the right by ρ^2 (which is the inverse of ρ) to obtain

$$\rho\sigma = \sigma\rho^2.$$

It is now clear that D_3 has at most 6 elements; namely, $\sigma^j\rho^k$ with $j \in \{0,1\}$ and $k \in \{0,1,2\}$. We show that these six names are distinct functions by showing that they do six different rigid motions to T:

element	action
id	identity
ρ	rotation by 120 degrees
ρ^2	rotation by 240 degrees
σ	reflection across the x-axis
$\sigma\rho$	reflection across the line which joins Q to the origin
$\sigma\rho^2$	reflection across the line which joins R to the origin

Here is the multiplication table for D_3.

	id	ρ	ρ^2	σ	$\sigma\rho$	$\sigma\rho^2$
id	id	ρ	ρ^2	σ	$\sigma\rho$	$\sigma\rho^2$
ρ	ρ	ρ^2	id	$\sigma\rho^2$	σ	$\sigma\rho$
ρ^2	ρ^2	id	ρ	$\sigma\rho$	$\sigma\rho^2$	σ
σ	σ	$\sigma\rho$	$\sigma\rho^2$	id	ρ	ρ^2
$\sigma\rho$	$\sigma\rho$	$\sigma\rho^2$	σ	ρ^2	id	ρ
$\sigma\rho^2$	$\sigma\rho^2$	σ	$\sigma\rho$	ρ	ρ^2	id

(12) Suppose H and K are subgroups of the group G. Is the intersection $H \cap K$ always a subgroup of G? If so, prove the statement. If not, give an example.

Answer: Yes, the intersection of H and K is a subgroup of G. We need only show that $H \cap K$ is non-empty, is closed under the operation of G, and if g is in $H \cap K$, then the inverse of g in G is also in $H \cap K$.

Let $*$ denote the operation in G.

Well, if g and g' are in $H \cap K$, then g and g' are in H and H is closed; so $g * g' \in H$. Similarly g and g' are in K and K is closed; so $g * g' \in K$. Thus $g * g' \in H \cap K$.

Let g be in $H \cap K$, let g_1 be the inverse of g in G. The hypothesis that H is a subgroup of G ensures that g_1 is in H. Similarly, the hypothesis that H is a subgroup of G ensures that g_1 is in K. Thus, g_1 is in $H \cap K$.

(13) Suppose H and K are subgroups of the group G. Is the union $H \cup K$ a always subgroup of G? If so, is prove the statement. If not, give an example.

Answer: The union of H and K is not always a subgroup of G. Consider the Klein four group of problem 5, call it G. The subgroup $\langle A \rangle$ is equal to $\{I, A\}$ and the subgroup $\langle B \rangle$ is equal to $\{I, B\}$. However the union

$$\langle A \rangle \cup \langle B \rangle = \{I, A, B\}$$

is not a group because $\{I, A, B\}$ is not closed under multiplication. Indeed, $AB = C \notin \{I, A, B\}$

(14) Let G be the group of rational numbers, under addition, and let H and K be subgroups of G. Prove that if $H \neq \{0\}$ and $K \neq \{0\}$, then $H \cap K \neq \{0\}$.

Answer: The hypotheses guarantee that there are positive intgers a, b, c, d with $h = \frac{a}{b} \in H$ and $k = \frac{c}{d} \in K$. Observe that

$$cbh = \underbrace{h + \cdots + h}_{cb \text{ times}} \quad \text{and} \quad adk = \underbrace{k + \cdots + k}_{ad \text{ times}}$$

are both equal to ac, which is a non-zero element of $H \cap K$.

(15) Let G be a group, and let $a \in G$. The set $C(a) = \{x \in G \mid xa = ax\}$ of all elements of G that commute with a is called the *centralizer* of a.

(a) Prove that $C(a)$ is a subgroup of G.

Answer: The identity element of G is in $C(a)$.
We show that $C(a)$ is closed. If x and y are elements of $C(a)$, then

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy);$$

hence $xy \in C(a)$.
We show that if $x \in C(a)$, then the inverse of x in G is also in $C(a)$. If $x \in C(a)$, then $xa = ax$ multiply both sides of the equation on the left by x^{-1} and multiply both sides of the equation on the right by a^{-1} to obtain $ax^{-1} = x^{-1}a$; hence x^{-1} is in $C(a)$.

(b) Prove that $\langle a \rangle \subseteq C(a)$.

Answer: This is obvious because a commutes with a; so $a \in C(a)$, but $C(a)$ is a group and $\langle a \rangle$ is the smallest subgroup of G which contains a; so all of $\langle a \rangle$ must be included in $C(a)$.

(c) Find the centralizer of ρ in D_4.

Answer: The centralizer of ρ in D_4 is $\langle \rho \rangle$. (Look at the multiplication table in the class notes if necessary.)

(d) Find the centralizer of ρ^2 in D_4.

Answer: The centralizer of ρ^2 in D_4 is D_4. (Look at the multiplication table in the class notes if necessary.)

(e) Find the centralizer in $\mathrm{GL}_2(\mathbb{R})$ of the matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Answer: The centralizer of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbb{R})$ is

$$\left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| \, a, b \in \mathbb{R} \text{ and } a \neq 0 \right\}.$$

Indeed each element from the proposed answer is in $\mathrm{GL}_n(\mathbb{R})$ and commutes with $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$:

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & b\\ 0 & a\end{bmatrix} = \begin{bmatrix}a & a+b\\ 0 & a\end{bmatrix}$$

and

$$\begin{bmatrix}a & b\\ 0 & a\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}a & a+b\\ 0 & a\end{bmatrix}.$$

Furthermore, if $\begin{bmatrix}a & b\\ c & d\end{bmatrix}$ is in $C\left(\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\right)$, then $ad-bd\neq 0$ and

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}.$$

Thus, $ad-bc\neq 0$ and

$$\begin{bmatrix}a+c & b+d\\ c & d\end{bmatrix} = \begin{bmatrix}a & a+b\\ c & c+d\end{bmatrix}$$

Thus,

$$ad-bc\neq 0,\quad a+c=a,\quad b+d=a+b,\quad c=c,\quad \text{and}\quad d=d+c.$$

Thus, $a\neq 0$, $c=0$, $a=d$.

(16) Find 6 subgroups of D_4 in addition to D_4 and $\{\mathrm{id}\}$.

Answer: The subgroups $\langle\rho^2\rangle$, $\langle\sigma\rho\rangle$, $\langle\sigma\rho^2\rangle$, $\langle\sigma\rho^3\rangle$, all have order 2. The subgroups $\langle\rho\rangle$ and $\langle\rho^2,\sigma\rangle$ both have order 4. The subgroup $\langle\rho\rangle$ is cyclic. The subgroup $\langle\rho^2,\sigma\rangle$ is not cyclic.

(17) Let U_8 be the group of complex numbers which satisfy $x^8=1$. Find two subgroups of U_8 in addition to $\{\mathrm{id}\}$ and U_8.

Answer: The subgroup $\langle i\rangle$ has order 4. The subgroup $\langle -1\rangle$ has order 2.

(18) Let G be the group U_9, which consists of all complex numbers z such that $z^9=1$.

(a) What is the order of each element of G?

Answer:

element	order
1	1
$e^{(2\pi i)/9}$	9
$e^{(4\pi i)/9}$	9
$e^{(6\pi i)/9}$	3
$e^{(8\pi i)/9}$	9
$e^{(10\pi i)/9}$	9
$e^{(12\pi i)/9}$	3
$e^{(14\pi i)/9}$	9
$e^{(16\pi i)/9}$	3

(b) Which elements of G are generators of all of G. (Recall that the element g in the group G *generates* G, if $\langle g \rangle = G$.)

Answer: Each of the elements $e^{(2\pi i)/9}$, $e^{(4\pi i)/9}$, $e^{(8\pi i)/9}$, $e^{(10\pi i)/9}$, $e^{(14\pi i)/9}$, and $e^{(16\pi i)/9}$ is a generator of G. These elements all have order 9. The other elements of G have order 1 or 3.

(c) Which elements g of G can be written in the form h^2 for some $h \in G$?

Answer: Every element of G can be written as h^2 for some h in G:

$g \in G$	$= h^2$ for some $h \in G$
1	$(1)^2$
$e^{(2\pi i)/9}$	$\left(e^{(10\pi i)/9}\right)^2$
$e^{(4\pi i)/9}$	$\left(e^{(2\pi i)/9}\right)^2$
$e^{(6\pi i)/9}$	$\left(e^{(12\pi i)/9}\right)^2$
$e^{(8\pi i)/9}$	$\left(e^{(4\pi i)/9}\right)^2$
$e^{(10\pi i)/9}$	$\left(e^{(14\pi i)/9}\right)^2$
$e^{(12\pi i)/9}$	$\left(e^{(6\pi i)/9}\right)^2$
$e^{(14\pi i)/9}$	$\left(e^{(16\pi i)/9}\right)^2$
$e^{(16\pi i)/9}$	$\left(e^{(8\pi i)/9}\right)^2$

(d) Which elements g of G can be written in the form h^3 for some $h \in G$?

Answer: The elements 1, $e^{(6\pi i)/9}$, and $e^{(12\pi i)/9}$ can be written in the form h^3 for some $h \in G$; but no other element of g can be written in this form.

$h \in G$	h^3
1	1
$e^{(2\pi i)/9}$	$e^{(6\pi i)/9}$
$e^{(4\pi i)/9}$	$e^{(12\pi i)/9}$
$e^{(6\pi i)/9}$	1
$e^{(8\pi i)/9}$	$e^{(6\pi i)/9}$
$e^{(10\pi i)/9}$	$e^{(12\pi i)/9}$
$e^{(12\pi i)/9}$	1
$e^{(14\pi i)/9}$	$e^{(6\pi i)/9}$
$e^{(16\pi i)/9}$	$e^{(12\pi i)/9}$

(19) Let H be a subgroup of the integers under addition. Prove that H is a cyclic group.

Answer: If $H = \{0\}$, then H is clearly cyclic. Henceforth, we assume that H is not $\{0\}$. In this case, H has some non-zero element h in it. The inverse of h, which is $-h$ is also in H. Thus, h has a positive element in it. Let h_0 be the smallest positive element in H. We claim that $H = \langle h_0 \rangle$. If h is any element of H, then (by the division algorithm) $h = ah_0 + b$ for integers[5] a and b with $0 \leq b \leq h_0 - 1$. Notice that $h \in H$ and ah_0 are both in H; hence b is in H. We chose h_0 to be the smallest positive integer in H. We see that $b < h_0$. We conclude that b is not positive; that is, b must be zero. Hence $h = ah_0$ and $H = \langle h_0 \rangle$.

(20) Find three subgroups of D_4 of order 4. (A subgroup of order 4 is a subgroup with 4 elements.)

Answer: The subgroups

$$\{\rho, \rho^2, \rho^3, \mathrm{id}\}, \quad \{\rho^2, \sigma, \sigma\rho^2, \mathrm{id}\}, \quad \text{and} \quad \{\sigma\rho, \sigma\rho^3, \rho^2, \mathrm{id}\}$$

of D_4 have order 4. The first subgroup is equal to the rotation group Rot_4. The second group was introduced in class as a copy of the Klein 4-group in D_4. The third group is the centralizer of $\sigma\rho$ in D_4. This is easy to check using the multiplication table for D_4.

(21) Let g be an element of the group G and let

$$S = \{n \in \mathbb{Z} \mid g^n = \mathrm{id}\}. \tag{0.0.1}$$

(In other words, S is the set of integers n such that g^n is equal to the identity of G.) Prove that S is a subgroup of $(\mathbb{Z}, +)$.

[5]Remember that ah_0 means $\underbrace{h_0 + \cdots + h_0}_{a \text{ times}}$ if a is positive; ah_0 means 0 if a is zero; and ah_0 means $\underbrace{(-h_0) + \cdots + (-h_0)}_{a \text{ times}}$ if a is negative. Keep in mind that the ambient group is the group of integers under addition.

(22) Consider $g = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ in the group $\mathrm{GL}_2(\mathbb{C})$. What is the set S (as in (0.0.1)) for g?

(23) Consider $g = \cos\frac{2\pi}{10} + i\sin\frac{2\pi}{10}$ in the unit circle group U. What is the set S (as in (0.0.1)) for g?

(24) Let $(G,*)$ be a group and let $H = \{g \in G \mid g*g*g = \mathrm{id}\}$. Calculate H for $G = D_4$, $G = D_3$, and $G = U_6$. (Recall that U_6 is the set of complex numbers which are sixth roots of 1.)

(25) Let G be a group. Suppose that g^2 is equal to the identity element of G for all g in G. Prove that G is an Abelian group.

(26) Let G be a finite group with an even number of elements. Prove that there must exist an element g of G with g not the identity element, but g^2 equal to the identity element.

(27) Find an example of a group G and elements a and b in G such that a and b each have finite order, but ab does not. (The element a of the group G has *finite order* if there exists a positive integer n with a^n equal to the identity element. If a does not have finite order, then a has *infinite order*.)

Answer: I have three answers.

Answer 1. Let $\mathscr{G}$ be the group of rigid motions of the plane with operation composition. Let σ be reflection across the x-axis and ρ be rotation fixing the origin by 1-radian. Notice that σ has order two and ρ has infinite order. Notice also that $\sigma\rho$ is a reflection; so $\sigma\rho$ has order two. Thus, σ and $\sigma\rho$ each have order two, but $\sigma(\sigma\rho) = \rho$ has infinite order.

Answer 2. Let $\mathscr{G}$ be the group of rigid motions of the plane with operation composition; let ℓ_1 and ℓ_2 be parallel lines in the plane; and let σ_i be reflection across ℓ_i. Observe that σ_1 and σ_2 have order two; but $\sigma_1\sigma_2$ is translation which has infinite order.

Answer 3. Let G be the group $\mathrm{GL}(2,\mathbb{R})$, $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$. Calculate A has order 2; B has order 4, but $AB = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ has infinite order. Indeed, $(AB)^n = \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix}$, where the f's are the Fibonacci numbers: $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_n + f_{n+1}$ for $0 \le n$.

(28) Let $G = D_4$ and let H be the subgroup of G which is generated by σ. List the left cosets of H in G.

Answer: The left cosets of H in G are:

$$\mathrm{id}\,H = \{\mathrm{id}, \sigma\}, \quad \rho H = \{\rho, \sigma\rho^3\}, \quad \rho^2 H = \{\rho^2, \sigma\rho^2\}, \quad \text{and} \quad \rho^3 H = \{\rho^3, \sigma\rho\}.$$

(29) Let $G = U_9$ and let H be the subgroup of G which is generated by u^3, where $u = \cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$. List the left cosets of H in G.

Answer: The left cosets of H in G are

$$\mathrm{id}H = \{id, u^3, u^6\}, \quad uH = \{u, u^4, u^7\}, \quad \text{and} \quad u^2H = \{u^2, u^5, u^8\}.$$

(30) Let G be the group $(\mathbb{R}^2, +)$, which consists of all column vectors with two real entries, under the operation of addition, and let H be the subgroup of G which consists of all elements of the form $\begin{bmatrix} a \\ a \end{bmatrix}$, for some real number a. Notice that each element of G corresponds in a natural way to a point in the xy-plane. Describe the left cosets of H in G.

Answer: The left cosets of H in G are

$$\left\{ \begin{bmatrix} b \\ 0 \end{bmatrix} + H \,\middle|\, b \in \mathbb{R} \right\}$$

We partition the xy-plane into lines parallel to the line $y = x$. The coset $\begin{bmatrix} b \\ 0 \end{bmatrix} + H$ is the line with slope 1 which passes through "$(b,0)$". (In my geometric description, I am identifying the vector $\begin{bmatrix} b+a \\ a \end{bmatrix}$ with the point $(a+b, b)$ which sits on the usual xy-plane.)

(31) Let G be a group. The set $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$ of all elements that commute with every other element of G is called the *center* of G.

(a) Prove that $Z(G)$ is a subgroup of G.
(b) Show that $Z(G) = \bigcap_{a \in G} C(a)$.
(c) Find the center of D_3.
(d) Find the center of D_4.
(e) Find the center of $\mathrm{GL}_2(\mathbb{R})$.

(32) Let G be a cyclic group. Let a and b be elements of G such that $a \neq g^2$ for any $g \in G$ and $b \neq g^2$ for any $g \in G$. Prove that ab is equal to g^2 for some $g \in G$. What happens if the hypothesis that G is a cyclic group is removed? Is the statement still true? If so, prove it. If not, find a counterexample. Recall that the group G is *cyclic* if there is an element h in G such that every element of G has the form h^n for some integer n.

(33) Let a and b be elements of a group G. Suppose that a and b both have finite order that the orders of a and b are relatively prime. Suppose further that $ab = ba$. Prove that the order of ab is equal to the order of a times the order of b. Recall that the *order* of a group element a is the least positive integer n with a^n equal to the identity element.

Answer: Let n be the order of a and m be the order of b. Use the hypothesis that a and b commute to see that

$$(ab)^{nm} = \underbrace{(ab)(ab)\cdots(ab)}_{nm \text{ times}} = a^{mn}b^{mn} = (a^n)^m(b^m)^n = \mathrm{id}.$$

Now we must show that nm is the smallest positive power which sends ab to the identity. Suppose the order of ab is c. The elements a and b commute; hence

$$a^c b^c = (ab)^c = \mathrm{id};$$

thus,

$$a^c = b^{-c} \in \langle a \rangle \cap \langle b \rangle.$$

The order of a^c divides the order of $\langle a \rangle$, which is n. The order of a^c also divides the order of $\langle b \rangle$, which is m. Hence, the order of a^c is a common divisor of n and m. On the other hand, the greatest common divisor of m and n is 1. Thus a^c has order 1; in other words, a^c is equal to the identity and n divides c.

In a similar manner, b^{-c} (which equals a^c) is also the identity; hence b^c is equal to the identity; so m divides c.

The numbers n and m are relatively prime and both numbers divide c. It follows that c is at least as large as nm.

(34) True or False. If true, prove it. If false, give a counterexample. Let G be a group and let H be the subset $H = \{g \in G \mid g^2 = \mathrm{id}\}$. Then H is a subgroup of G.

(35) (a) Compute the left and right cosets of $H = \langle \sigma \rangle$ in $G = D_3$.
(b) Is ghg^{-1} in H for all $g \in G$ and h in H, where H and G are as given in (a)?
(c) Compute the left and right cosets of $H = \langle \rho \rangle$ in $G = D_3$.
(d) Is ghg^{-1} in H for all $g \in G$ and h in H, where H and G are as given in (c)?

Answer:

(a) The left cosets of $\langle \sigma \rangle$ in D_3 are $\{\mathrm{id}, \sigma\}$, $\{\rho, \sigma\rho^2\}$, and $\{\rho^2, \sigma\rho\}$.

The right cosets of $\langle \sigma$ in D_3 are $\{\mathrm{id}, \sigma\}$, $\{\rho, \sigma\rho\}$, and $\{\rho^2, \sigma\rho^2\}$.

(b) No, $\rho\sigma\rho^{-1} = \rho\sigma\rho^2 = \sigma\rho \notin H$.

(c) The left and right cosets of $\langle \rho \rangle$ in D_3 are $\{\mathrm{id}, \rho, \rho^2\}$ and $\{\sigma, \sigma\rho, \sigma\rho^2\}$

(d) Yes. It is obvious that $gHg^{-1} \in H$, when $g \in H$. We check the three elements of G which are not in H:

$$\sigma H \sigma^{-1} = \{\sigma\,\mathrm{id}\,\sigma, \sigma\rho\sigma, \sigma\rho^2\sigma\} = \{\mathrm{id}, \rho^2, \rho\} = H,$$

$$\sigma\rho H(\sigma\rho)^{-1} = \{(\sigma\rho)\,\mathrm{id}(\rho^2\sigma), (\sigma\rho)\rho(\rho^2\sigma), (\sigma\rho)\rho^2(\rho^2\sigma)\} = \{\mathrm{id}, \rho^2, \rho\} = H,$$

$$\sigma\rho^2 H(\sigma\rho^2)^{-1} = \{(\sigma\rho^2)\,\mathrm{id}(\rho\sigma), (\sigma\rho^2)\rho(\rho\sigma), (\sigma\rho^2)\rho^2(\rho\sigma)\} = \{\mathrm{id}, \rho^2, \rho\} = H,$$

(36) (a) Suppose that H is a subgroup of the group G with the property that ghg^{-1} in H for all $g \in G$ and h in H. Let a, b, and c be elements of G with $aH = bH$, prove that $acH = bcH$.

(b) Suppose that H is a subgroup of the group G and that a, b, and c be elements of G with $aH = bH$. Must $acH = bcH$? Prove or give a counterexample.

Answer: (36a) We are told that $aH = bH$. It follows that $a = bh$ for some h in H. Therefore,

$$acH = bhcH = bc(c^{-1}hc)hH.$$

The element $c^{-1}hc$ is in H by hypothesis; hence $(c^{-1}hc)h \in H$ and $bc(c^{-1}hc)hH = bcH$. We conclude that $acH = bcH$.

(36b) Let $G = D_3$, $H = \langle \sigma \rangle$, $a = \mathrm{id}$, $b = \sigma$, and $c = \sigma\rho$.

Observe that $aH = bH$ (that is $\mathrm{id}\,H = \sigma H$),

$$acH = \mathrm{id}\,\sigma\rho H = \{\sigma\rho, \sigma\rho\sigma\} = \{\sigma\rho, \rho^2\},$$

and

$$bcH = \sigma\sigma\rho H = \rho H = \{\rho, \rho\sigma\} = \{\rho, \sigma\rho^2\}.$$

In particular, $aH = bH$; however, $acH \neq bcH$.

(37) Let G be $(\mathbb{C} \setminus \{0\}, \times)$. Describe the left cosets of the subgroup H in G where

(a) $H = U_4$

(b) $H = \{ru \mid r \text{ is a positive real number and } u \in U_4\}$.

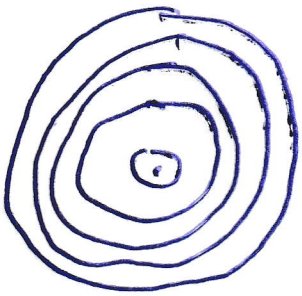
Answer:

(37a) For each positive real number r and each angle θ with $0 \leq \theta < \frac{\pi}{2}$, the left coset $re^{i\theta}U_4$ consists of four points: $re^{i\theta}$, $ire^{i\theta}$, $-re^{i\theta}$, and $-ire^{i\theta}$.

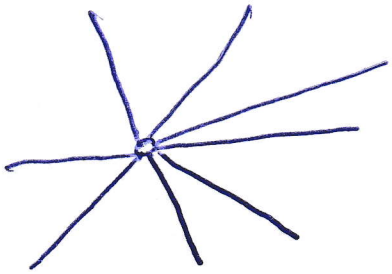
(37b) For each θ with $0 \leq \theta < \frac{\pi}{2}$, the coset $e^{\theta i}H$ consists of four rays eminating from the origin: one ray makes the angle θ with the positive x-axis, one ray makes the angle θ with the positive y-axis, one ray makes the angle θ with the negative x-axis, and the final ray makes the angle θ with the negative y-axis.

Here is a solution to Questions 3.11 and 3.12 from the class notes.

3.11 Each left coset of U in $(\mathbb{C}^\times, \times)$ has the form rU for some positive real number R. These cosets partition the complex plane (without zero) into concentric circles



3.12 Each left coset of $(\mathbb{R}^{pos}, \times)$ in $(\mathbb{C}^\times, \times)$ has the form $e^{i\theta}\mathbb{R}^{pos}$ for some real θ with $0 \leq \theta < 2\pi$. These cosets partition the complex plane (without 0) into rays emanating from 0



(38) Suppose that H is a subgroup of the group G and ghg^{-1} is in H for all $g \in G$ and $h \in H$.

(a) Let h_1 be an arbitrary element of H and g be an arbitrary element of G. Prove that there exists an element h of H with $h_1 = ghg^{-1}$. (It is possible to give a proof which works for infinite groups as well as finite groups.)

(b) Let a, b, c, and d be elements of G with $aH = bH$ and $cH = dH$. Prove that $acH = bdH$.

(c) Let S be the set of cosets $S = \{aH \mid a \in G\}$ of H in G. Problem 38b shows that the operation on S given by $(aH) * (bH) = abH$ is a well-defined function. Prove that S is a group. (If you are looking for this somewhere, S is usually written as $\frac{G}{H}$ and S is called the "quotient group of G mod H", or the "factor group of G mod H". BY THE WAY: S is not a subset of anything; we have to verify all of the axioms for group. Fortunately, this is very easy.)

Answer: (38a) Let h_1 be an arbitrary element of H and g be an arbitrary element of G. The hypothesis guarantees that $h = g^{-1}h_1g \in H$. Observe that

$$ghg^{-1} = g(g^{-1}h_1g)g^{-1} = h.$$

(38b) The cosets aH and bH are equal; so there is an element $h_1 \in H$ with $a = bh_1$; and the cosets cH and dH are equal; so there is an element $h_2 \in H$ with $c = dh_2$. Thus,

$$acH = bh_1cH = bc(c^{-1}h_1c)H.$$

The ambient hypothesis ensures that $c^{-1}hc \in H$. It follows that

$$acH = bcH = bdh_2H = bdH.$$

(38c) The identity element of S is $\mathrm{id}\,H$ because if aH is any element of S, then $\mathrm{id}\,H * aH = \mathrm{id}\,aH = aH$ and $aH * \mathrm{id}\,H = a\,\mathrm{id}\,H = aH$.

The operation in S is closed: if a and b are elements of G, then aH and bH are elements of H and $aH * bH$ is equal to abH which is an element of S.

The operation in S associates: if a, b, and c are elements of G, then aH, bH and cH are elements of S and

$$(aH * bH) * cH = (abH) * cH = ((ab)c) * H = (a(bc)) * H = (aH) * (bcH) = aH * (bH * cH).$$

The inverse of aH is $a^{-1}H$ where a^{-1} is the inverse in G of the element a of G.

(39) (a) If G is an Abelian group and H is a subgroup of G, then prove that ghg^{-1} is in H for all $g \in G$ and $h \in H$.

(b) If G is a finite group with $2n$ elements and H is a subgroup of G with n elements, then prove that ghg^{-1} is in H for all $g \in G$ and $h \in H$.

(c) If G is a group and H is a subgroup of the center of G, then prove that ghg^{-1} is in H for all $g \in G$ and $h \in H$. (The word center is defined in Problem 31.)

For future reference, a subgroup H of a group G is called a *normal* subgroup if ghg^{-1} is in H for all $g \in G$ and $h \in H$.

Answer: Assertion (39a) is easy. If $g \in G$, $h \in H$, and G is Abelian, then $ghg^{-1} = hgg^{-1} = h_1 \in H$.

Assertion (39c) is just as easy as (39a). We are given $g \in G$ and $h \in H$. We are told that each element of H commutes with every element of G. Once again, $ghg^{-1} = hgg^{-1} = h \in H$.

Assertion (39b) is more subtle. We argue by contradiction. Suppose $g \in G$ and $h \in H$ with $ghg^{-1} \notin H$. One consequence of our hypothesis (that $ghg^{-1} \notin H$) is that $g \notin H$. But there are exactly two left cosets of H in G. They are H and gH. Thus, $G = H \cup gH$.

We have assumed that $ghg^{-1} \notin H$. It follows that $ghg^{-1} \in gH$. In other words, there is an element $h_1 \in H$ with $ghg^{-1} = gh_1$. Observe that the most recent equation forces $hg^{-1} = h_1$ and $h_1^{-1}h = g$. This is a contradiction because $g \notin H$ and $h_1^{-1}h$ is in H.

(40) Work out some examples of $\frac{G}{H}$ as described in problem 38c.

(a) Let $G = D_4$ and $H = \langle \rho \rangle$. Problem 39c tells us that it is legal to create $\frac{G}{H}$. What is this group? How many elements does it have? What is the multiplication table? Do you believe that this multiplication makes sense?

(b) Let $G = D_4$ and $H = \langle \rho^2 \rangle$. Problem 39b tells us that it is legal to create $\frac{G}{H}$. What is this group? How many elements does it have? What is the multiplication table? Do you believe that this multiplication makes sense?

(c) Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$. Problem 39a tells us that it is legal to create $\frac{G}{H}$. What is this group? How many elements does it have? What is the addition table? Do you believe that this addition makes sense? (Notice that the elements of this $\frac{G}{H}$ look like $a+H$ because the operation in G is called $+$. Furthermore, the operation in $\frac{G}{H}$ is also called $+$; that is, $(a+H)+(b+H) = a+b+H$.)

Answer: (40a) The group $\frac{D_4}{\langle \rho \rangle}$ has two elements: $\mathrm{id} * \langle \rho \rangle$ and $\sigma * \langle \rho \rangle$. The group $\frac{D_4}{\langle \rho \rangle}$ is the cyclic group of order two. The multiplication table is

	$\mathrm{id}*\langle\rho\rangle$	$\sigma*\langle\rho\rangle$
$\mathrm{id}*\langle\rho\rangle$	$\mathrm{id}*\langle\rho\rangle$	$\sigma*\langle\rho\rangle$
$\sigma*\langle\rho\rangle$	$\sigma*\langle\rho\rangle$	$\mathrm{id}*\langle\rho\rangle$

(40b) The group $\frac{D_4}{\langle\rho^2\rangle}$ has four elements: $\mathrm{id}*\langle\rho^2\rangle$, $\sigma*\langle\rho^2\rangle$, $\sigma\rho*\langle\rho^2\rangle$, and $\rho*\langle\rho^2\rangle$. The group is a Klein 4-group.

	$\mathrm{id}*\langle\rho^2\rangle$	$\sigma*\langle\rho^2\rangle$	$\sigma\rho*\langle\rho^2\rangle$	$\rho*\langle\rho^2\rangle$
$\mathrm{id}*\langle\rho^2\rangle$	$\mathrm{id}*\langle\rho^2\rangle$	$\sigma*\langle\rho^2\rangle$	$\sigma\rho*\langle\rho^2\rangle$	$\rho*\langle\rho^2\rangle$
$\sigma*\langle\rho^2\rangle$	$\sigma*\langle\rho^2\rangle$	$\mathrm{id}*\langle\rho^2\rangle$	$\rho*\langle\rho^2\rangle$	$\sigma\rho*\langle\rho^2\rangle$
$\sigma\rho*\langle\rho^2\rangle$	$\sigma\rho*\langle\rho^2\rangle$	$\rho*\langle\rho^2\rangle$	$\mathrm{id}*\langle\rho^2\rangle$	$\sigma*\langle\rho^2\rangle$
$\rho*\langle\rho^2\rangle$	$\rho*\langle\rho^2\rangle$	$\sigma\rho*\langle\rho^2\rangle$	$\sigma*\langle\rho^2\rangle$	$\mathrm{id}*\langle\rho^2\rangle$

(40c) The group $\frac{\mathbb{Z}}{5\mathbb{Z}}$ is the cyclic group with five elements. The operation table is

	$0+5\mathbb{Z}$	$1+5Z$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$0+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5Z$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5Z$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5Z$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5Z$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5Z$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$

(41) Prove that if N is a normal subgroup of the group G, and H is any subgroup of G, then $H\cap N$ is a normal subgroup of H. The word normal is defined in problem 39.

Answer: The intersection of the two subgroups H and N of G is a subgroup of G by HW 11. It follows that $H\cap N$ is a subgroup of G and also a subgroup of H. We will show that $H\cap N$ is a **normal** subgroup of H. That is, we will show that if $h\in H$ and $x\in H\cap N$, then hxh^{-1} is in $H\cap N$. Of course, this is obvious. Indeed, h, x, and h^{-1} are in H and H is a group; so hxh^{-1} is in H. Also, N is a normal subgroup of G, $n\in N$ and $h\in H\subseteq G$. It follows that $hnh^{-1}\in N$. We have shown that hnh^{-1} is in H and hnh^{-1} is in N. We conclude that hnh^{-1} is in $H\cap N$.

(42) Let G be a finite group, and let n be a divisor of $|G|$. Prove that if H is the only subgroup of G of order n , then H must be normal in G . (The symbol $|G|$ means the number of elements in the group G. It is often read as the *order* of G.)

Answer: Let g be a fixed, but arbitrary, element of G. Observe that gHg^{-1} is a subgroup of G of order n. The hypothesis ensures that H is the only subgroup of G of order n. It follows that $gHg^{-1}=H$. Indeed, $gHg^{-1}=H$ for all $g\in G$; therefore H is a normal subgroup of G.

(43) Let H and K be normal subgroups of of the group G such that $H \cap K = \langle \mathrm{id} \rangle$ Prove that $hk = kh$ for all $h \in H$ and $k \in K$.

(44) Prove that $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(0,1)\rangle}$ is an infinite cyclic group. Recall that the direct product of $\mathbb{Z}$ with $\mathbb{Z}$ is the group of ordered pairs (a,b), where a and b are integers. The operation is coordinate wise addition: $(a,b)+(c,d) = (a+c,b+d)$, for integers a, b, c, and d. (For a more sophisticated solution to this problem than you are able to give now, see problem 71.)

(45) Prove that $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(1,1)\rangle}$ is an infinite cyclic group. (For a more sophisticated solution to this problem than you are able to give now, see problem 72.)

(46) Prove that $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(2,2)\rangle}$ is not a cyclic group.

(47) Compute the group

$$\frac{\frac{Z}{\langle 6\rangle} \times \frac{\mathbb{Z}}{\langle 4\rangle}}{\langle(\bar{2},\bar{2})\rangle}.$$

(For a more sophisticated solution to this problem than you are able to give now, see problem 73.)

(48) Compute the group

$$\frac{\frac{Z}{\langle 6\rangle} \times \frac{\mathbb{Z}}{\langle 4\rangle}}{\langle(\bar{3},\bar{2})\rangle}.$$

(49) Find all cyclic subgroups of $\frac{\mathbb{Z}}{\langle 8\rangle}$.

Answer: The group $\frac{\mathbb{Z}}{\langle 8\rangle}$ is cyclic of order 8. We proved that every subgroup of a cylic group is cyclic. We also proved that a cyclic group of order n has exactly one subgroup for each divisor d of n. Indeed, if g has order n, then $\langle g^{n/d}\rangle$ is the subgroup of $\langle g\rangle$ of order d. The group $\frac{\mathbb{Z}}{\langle 8\rangle}$ has four subgroups. Each of the subgroups is cyclic.

The subgroup generated by $1+\langle 8\rangle$ has order 8 and is equal to $\frac{\mathbb{Z}}{\langle 8\rangle}$.

The subgroup generated by $2+\langle 8\rangle$ has order 4 and is equal to

$$\{2+\langle 8\rangle, 4+\langle 8\rangle, 6+\langle 8\rangle, 0+\langle 8\rangle\}.$$

The subgroup generated by $4+\langle 8\rangle$ has order 2 and is equal to

$$\{4+\langle 8\rangle, 0+\langle 8\rangle\}.$$

The subgroup generated by $0+\langle 8\rangle$ has order 1 and is equal to

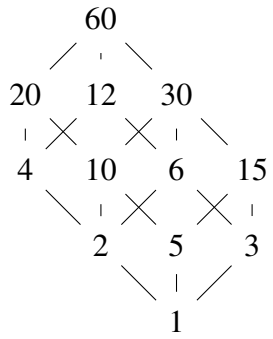
$$\{0+\langle 8\rangle\}.$$

(50) Give a subgroup diagram of $\frac{\mathbb{Z}}{\langle 60\rangle}$.

The group $\frac{\mathbb{Z}}{\langle 60\rangle}$ is cyclic of order 60 generated by the coset $1+\langle 60\rangle$. We proved that every subgroup of a cylic group is cyclic. We also proved that a cyclic group of order n has exactly one subgroup for each divisor d of n. Indeed, if g has order n, then $\langle g^{n/d}\rangle$ is the subgroup of $\langle g\rangle$ of order d. The group $\frac{\mathbb{Z}}{\langle 60\rangle}$ has twelve subgroups; one for each divisor $1,2,3,4,5,6,10,12$,

$15, 20, 30, 60$ of 60. Each of the subgroups is cyclic. I found the following picture on the internet at

https://tex.stackexchange.com/questions/585941/using-tikzpicture-how-can-i-sketch-the-lattice-of-divisors-of-60



The picture represents the lattice of divisors of 60. There is a line between two divisors a and b (with $a < b$) provided a divides b (with $\frac{b}{a}$ prime). The same picture describes the lattice of subgroups of $\frac{\mathbb{Z}}{\langle 60\rangle}$ where a represents the subgroup of $\frac{\mathbb{Z}}{\langle 60\rangle}$ generated by the coset $a+\langle 60\rangle$. There is a line between two divisors a and b (with $a < b$) provided a divides b (with $\frac{b}{a}$ prime). The line between a and b indicates that the subgroup of $\frac{\mathbb{Z}}{\langle 60\rangle}$ generated by $b+\langle 60\rangle$ is a subgroup of the subgroup of $\frac{\mathbb{Z}}{\langle 60\rangle}$ generated by $a+\langle 60\rangle$.

(51) Find the cyclic subgroup of $(\mathbb{C}\setminus\{0\},\times)$ generated by $\frac{\sqrt{2}+i\sqrt{2}}{2}$.

(52) Find the order of the cyclic subgroup of $(\mathbb{C}\setminus\{0\},\times)$ generated by i.

(53) Find all cyclic subgroups of $\frac{\mathbb{Z}}{\langle 4\rangle}\times\frac{\mathbb{Z}}{\langle 2\rangle}$.

(54) Define $\varphi:(\mathbb{C}\setminus\{0\},\times)\to(\mathbb{R}\setminus\{0\},\times)$ by $\varphi(a+bi)=a^2+b^2$. Prove that φ is a homomorphism.

Answer: Let $a+bi$ and $c+di$ be non-zero complex numbers with a,b,c,d real. We compute that

$$\varphi(a+bi)\varphi(c+di)=(a^2+b^2)(c^2+d^2)$$

$$\begin{aligned}\varphi((a+bi)(c+di)) &= \varphi((ac-bd)+i(ad+bc)) = (ac-bd)^2+(ad+bc)^2\\ &= a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2d^2\\ &= a^2c^2+b^2c^2+a^2d^2+b^2d^2 = a^2(c^2+d^2)+b^2(c^2+d^2)\\ &= (a^2+b^2)(c^2+d^2).\end{aligned}$$

We get the same answer both times. We conclude that φ is a homomorphism.

(55) Which of the following are homomorphisms?

(a) $\varphi:(\mathbb{R}\setminus\{0\},\times)\to \mathrm{GL}_2(\mathbb{R})$ defined by $\phi(a)=\begin{bmatrix}a & 0\\ 0 & 1\end{bmatrix}$

Answer: This φ is a homomorphism. If a and b are non-zero real numbers, then

$$\varphi(ab) = \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$\varphi(a)\varphi(b) = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}.$$

(b) $\varphi : (\mathbb{R}, +) \to \mathrm{GL}_2(\mathbb{R})$ defined by $\phi(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$

Answer: This φ is a homomorphism. If a and b are real numbers, then

$$\varphi(a+b) = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

and

$$\varphi(a)\varphi(b) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}.$$

(c) $\varphi : \mathrm{Mat}_{2\times 2}(\mathbb{R}) \to (\mathbb{R}, +)$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a$,

Recall that $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is the Abelian group of 2×2 matrices with real number entries. The operation in $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is matrix addition.

Answer: This φ is a homomorphism. If

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

are matrices with real entries, then

$$\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}\right) = a+e$$

$$\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = a+e$$

(d) $\varphi : \mathrm{GL}_2(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ab$.

Answer: This φ is not a homomorphism. For example, if

$$A = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

then A and B are in $\mathrm{GL}_2(\mathbb{R})$, but

$$\varphi(AB) = \varphi(A) = 1; \text{ however } \varphi(A)\varphi(B) = 1(0) = 0.$$

Notice that $\varphi(B)$ is not even an element of the target of φ. The question does not even make sense!

(e) $\varphi : \mathrm{GL}_2(\mathbb{R}) \to (\mathbb{R}, +)$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d$

Answer: This φ is not a homomorphism. For example, if

$$A = B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

then A and B are in $\mathrm{GL}_2(\mathbb{R})$, but

$$\varphi(AB) = \varphi(A) = 2; \text{ however } \varphi(A) + \varphi(B) = 2 + 2 = 4.$$

(f) $\varphi : \mathrm{GL}_2(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$ defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc.$

Answer: This φ is a homomorphism. The determinant of a product is the product of the determinants. If the matrices are both invertible then their determinants are non-zero.
We can check this by hand. Take

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

from $\mathrm{GL}_2(\mathbb{R})$. Observe that

$$\begin{aligned} \varphi(AB) &= \varphi\left(\begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}\right) \\ &= (ae+bg)(cf+dh) - (af+bh)(ce+dg) \\ &= ae(cf+dh) - af(ce+dg) + bg(cf+dh) - bh(ce+dg) \\ &= aedh - afdg + bgcf - bhce \\ &= ad(eh-fg) - bc(eh-fg) \\ &= (ad-bc)(eh-fg) = \varphi(A)\varphi(B). \end{aligned}$$

Are you small?

(56) Let $\varphi : G_1 \to G_2$ and $\theta : G_2 \to G_3$ be group homomorphisms. Prove that $\theta \circ \varphi : G_1 \to G_3$ is a group homomorphism. Prove that $\ker(\varphi) \subseteq \ker(\theta \circ \varphi)$.

Answer: Let $*_i$ be the operation in G_i. Let g_1 and g_1' be elements of G_1. We compute

$$\begin{aligned} (\theta \circ \varphi)(g_1 *_1 g_1') &= \theta(\varphi(g_1 *_1 g_1')), && \text{this is the meaning of composition,} \\ &= \theta(\varphi(g_1) *_2 \varphi(g_1')), && \text{because } \varphi \text{ is a homomorphism,} \\ &= \theta(\varphi(g_1)) *_3 \theta(\varphi(g_1')), && \text{because } \theta \text{ is a homomorphism,} \\ &= (\theta \circ \varphi)(g_1)) *_3 (\theta \circ \varphi)(g_1'), && \text{this is the meaning of composition.} \end{aligned}$$

Thus,

$$(\theta \circ \varphi)(g_1 *_1 g_1') = (\theta \circ \varphi)(g_1)) *_3 (\theta \circ \varphi)(g_1'),$$

and the proof is complete.

The kernel of φ is the set of elements in the domain of φ which are sent to the identity element of the target of φ. Suppose g_1 is in the kernel of φ. Then

$$(\theta \circ \varphi)(g_1) = \theta(\mathrm{id}) = \mathrm{id}$$

because every group homomorphism carries the identity element of the source to the identity element of the target.

(57) Prove that the intersection of two normal subgroups of a group G is a normal subgroup of G.

(58) Let $\varphi : G \to G'$ be a group homomorphism.
   (a) Let id be the identity element of G and id' be the identity element of G'. Prove that $\varphi(\mathrm{id}) = \mathrm{id}'$.
   (b) Let g be an element of G. Prove that φ of the inverse of g is equal to the inverse of $\varphi(g)$.
   (c) The image of φ is the subset $\operatorname{im}\varphi = \{\varphi(g) \mid g \in G\}$ of G'. Prove that $\operatorname{im}\varphi$ is a subgroup of G'.
   (d) The kernel of φ is the subset $\ker\varphi = \{g \in G \mid \varphi(g) = \mathrm{id}'\}$, where id' is the identity element of G'. Prove that the kernel of φ is a subgroup of G.
   (e) Prove that $\ker\varphi$ is a normal subgroup of G.
   (f) Consider $\bar{\varphi} : \frac{G}{\ker\varphi} \to \operatorname{im}\varphi$, which is given by $\bar{\varphi}(g\ker\varphi) = \varphi(g)$. Prove that $\bar{\varphi}$ is a **FUNCTION**. That is, if $g_1\ker\varphi$ and $g_2\ker\varphi$ are equal cosets, then prove that $\bar{\varphi}(g_1\ker\varphi) = \bar{\varphi}(g_2\ker\varphi)$.
   (g) Prove that $\bar{\varphi}$ is a group homomorphism.
   (h) Prove that $\bar{\varphi}$ is onto.
   (i) Prove that $\bar{\varphi}$ is one-to-one.

In problem 58, you have proven the following very important Theorem.

The First Isomorphism Theorem *If $\varphi : G \to G'$ is a group homomorphism, then $\bar{\varphi} : \frac{G}{\ker\varphi} \to \operatorname{im}\varphi$, which is given by $\bar{\varphi}(g\ker\varphi) = \varphi(g)$, is a group isomorphism.*

(59) Let G be a cyclic group with generator g. Consider the function $\varphi : \mathbb{Z} \to G$ which is given by $\varphi(m) = g^m$ for all integers m.
   (a) Prove that φ is a group homomorphism.
   (b) Prove that φ is onto.
   (c) If G is infinite, then prove that φ is an isomorphism.
   (d) If G has finite order n, then prove that G is isomorphic to $\frac{\mathbb{Z}}{n\mathbb{Z}}$. (I strongly encourage you to use the First Isomorphism Theorem.)

(60) Let S and T be sets and let $\varphi : S \to T$ be a function. Suppose that φ is one-to-one and onto.
   (a) Prove that there exists a FUNCTION $\theta : T \to S$ with $\varphi\circ\theta$ equal to the identity function on T and $\theta\circ\varphi$ equal to the identity function on S. (The function θ is usually called the inverse of φ.)
   (b) Prove that the function θ of part (a) is one-to-one and onto.
   (c) If S and T happen to be groups and φ happens to be a group homomorphism, then prove that θ is also a group homomorphism.

(61) Let $\varphi : G \to G'$ and $\varphi' : G' \to G''$ be group homomorphisms. Prove that $\varphi'\circ\varphi : G \to G''$ is a group homomorphism.

(62) Prove that the relationship "is isomorphic to" is an equivalence relation on the class of all groups. Recall that a relation $\sim$ on a class C is an *equivalence relation* if
   (a) The relation $\sim$ is *reflexive*. If $c \in C$, then $c \sim c$.

(b) The relation $\sim$ is *symmetric*. If $c \sim c'$ for some c and c' in C, then $c' \sim c$.
(c) The relation $\sim$ is *transitive*. If $c \sim c'$ and $c' \sim c''$ for some c, c', c'' in C, then $c \sim c''$.

In problems 59 and 62, you have proven the following Theorem.

Theorem
(a) *If G and G' are infinite cyclic groups, then G and G' are isomorphic.*
(b) *If G and G' are cyclic groups of finite order n, then G and G' are isomorphic.*

(63) Let $\varphi : G \to G'$ be a group homomorphism. Prove that φ is one-to-one if and only if $\ker\varphi = \{\mathrm{id}\}$.

(64) Let m and n be non-zero integers and let H be the subset

$$H = \{am + bn \mid a, b \in \mathbb{Z}\}$$

of $\mathbb{Z}$.
(a) Prove that H is a subgroup of $\mathbb{Z}$.
(b) We have shown that every subgroup of $\mathbb{Z}$ is cyclic. So H is cyclic. Let h_0 be a generator of H. (We can insist that h_0 is positive.) Prove that h_0 is a common divisor of m and n.
(c) Suppose that ℓ is an integer which happens to divide m and n. Prove that ℓ must also divide h_0.
(d) Notice that you have proven that h_0 is the greatest common divisor of m and n.

In problem 64, you have proven the following result.

Lemma from Number Theory. *If d is the greatest common divisor of the non-zero integers m and n, then there exist integers r and s so that*

$$d = rn + sm.$$

Answer: We proved this in Lemma 4.6 in the class notes.

(65) Suppose m and n are relatively prime non-zero integers. Prove that the groups $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ and $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ are isomorphic. (An algebraist calls this result the Chinese Remainder Theorem.)

(66) Let G be a cyclic group of order n; let g be a generator of G; and let H be a subgroup of G of order m. Lagrange's Theorem tells us that $m|n$. Let d equal the integer $\frac{n}{m}$. I want you to prove that H is the subgroup of G which is generated by g^d. I propose a couple of steps. First of all, we know that H is cyclic, so $H = \langle g^r \rangle$ for some integer r.
(a) Prove that $d|r$.
(b) Now you know that $H = \langle g^r \rangle \subseteq \langle g^d \rangle$. Finish the proof that $H = \langle g^d \rangle$.

Answer: We proved this in Corollary 4.3.

(67) Define a group homomorphism from $\mathbb{Z} \times \mathbb{Z}$ onto $\mathbb{Z}$ whose kernel is the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by $(0, 1)$. Apply the First Isomorphism Theorem. (This problem gives a more sophisticated solution to problem 44 than you were able to give when you first did problem 44.)

(68) Define a group homomorphism from $\mathbb{Z}\times\mathbb{Z}$ onto $\mathbb{Z}$ whose kernel is the subgroup of $\mathbb{Z}\times\mathbb{Z}$ generated by $(1,1)$. Apply the First Isomorphism Theorem. (This problem gives a more sophisticated solution to problem 45 than you were able to give when you first did problem 45.)

(69) Consider $\varphi : \frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \to \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, given by

$$\varphi(a+6\mathbb{Z}, b+4\mathbb{Z}) = (a+3\mathbb{Z}, b+2\mathbb{Z}).$$

(a) Prove that φ is a function.
(b) Prove that φ is a group homomorphism.
(c) What are the image and kernel of φ?
(d) What does the First Isomorphism Theorem tell you?

Problem 69 gives a more sophisticated solution to problem 47 than you were able to give when you first did problem 47.

(70) Find a group homomorphism from $\mathbb{Z}\times\mathbb{Z}$ onto $\mathbb{Z}\times\frac{\mathbb{Z}}{2\mathbb{Z}}$, whose kernel is the subgroup of $\mathbb{Z}\times\mathbb{Z}$ which is generated by $(2,2)$. Apply the First Isomorphism Theorem.

(71) Exhibit an isomorphism $\phi : U \to G$, where U is the unit circle group and G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. Tell me what G is. Tell me what ϕ is. Prove that ϕ is an isomorphism.

(72) Exhibit an isomorphism $\varphi : (\mathbb{R}\setminus\{0\}, \times) \to (\mathbb{R}\setminus\{-2\}, *)$, where $a * b = ab + 2a + 2b + 2$. Tell me what ϕ is and prove that ϕ is an isomorphism.

Answer: Define φ by $\varphi(a) = a - 2$.

Observe that if $a \in \mathbb{R}\setminus\{0\}$, then $\varphi(a) \in (\mathbb{R}\setminus\{-2\}, *)$. Indeed, φ is obviously injective and surjective.

Observe also that if a and b are in the domain of φ, then

$$\varphi(ab) = ab - 2.$$

On the other hand,

$$\varphi(a) * \varphi(b) = (a-2) * (b-2) = (a-2)(b-2) + 2(a-2) + 2(b-2) + 2$$

$$= (ab - 2a - 2b + 4) + (2a - 4) + (2b - 4) + 2 = ab - 2 = \varphi(ab).$$

(73) Let $H = \{\mathrm{id}, a, b, c\}$ be a Klein 4-group with $a^2 = b^2 = c^2 = \mathrm{id}$, $ab = ba = c$, $ac = ca = b$, and $bc = cb = a$. The group H has exactly 4 elements. Consider the function $\varphi : \mathbb{Z}\times\mathbb{Z} \to H$ which is given by $\varphi(m,n) = a^m b^n$. Prove that φ is a group homomorphism. Prove that φ is onto. What is the kernel of φ? What does the First Isomorphism Theorem tell you?

(74) Is the additive group $\mathbb{C}$ isomorphic to the multiplicative group $(\mathbb{C}\setminus\{0\}, \times)$?

(75) Prove that every group with three elements is isomorphic to $\frac{\mathbb{Z}}{\langle 3\rangle}$.

(76) Find two Abelian groups of order 8 that are not isomorphic.

(77) Let C_2 be the subgroup $\{1, -1\}$ of $(\mathbb{R}\setminus\{0\}, \times)$. Prove that $(\mathbb{R}\setminus\{0\}, \times)$ is isomorphic to $(\mathbb{R}^{\mathrm{pos}}, \times) \times C_2$, where $\mathbb{R}^{\mathrm{pos}}$ is the set of positive real numbers.

(78) Recall the group $(S, *)$ of problem (7). Prove that $(S, *)$ is isomorphic to $(\mathbb{R}\setminus\{0\}, \times)$.

(79) Let G be a group, and let a be a fixed element of G. Define a function $\varphi_a : G \to G$ by $\varphi_a(x) = axa^{-1}$, for all $x \in G$. Prove that φ_a is an isomorphism.

(80) Let G be a group. Define $\varphi : G \to G$ by $\varphi(x) = x^{-1}$, for all $x \in G$.
   (a) Prove that φ is one-to-one and onto.
   (b) Prove that φ is an isomorphism if and only if G is Abelian.

(81) Define $\varphi : (\mathbb{C} \setminus \{0\}, \times) \to (\mathbb{C} \setminus \{0\}, \times)$ by $\varphi(a+bi) = a-bi$. Prove that φ is an isomorphism.

(82) Prove that $(\mathbb{C} \setminus \{0\}, \times)$ is isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{R})$ which consists of all matrices of the form

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

with $a^2 + b^2 \neq 0$.

(83) Recall the group G of problem (6). Prove that G is isomorphic to the group $(\mathbb{R} \setminus \{0\}, \times)$.

(84) Consider the following permutations in S_7:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}.$$

   (a) Compute $\sigma \circ \tau$.
   (b) Write $\sigma \circ \tau$ as a product of disjoint cycles.
   (c) Write σ and τ each as a product of transpositions.

Answer: (84a) Observe that $\sigma = \boxed{(1,3,5,6)}$, $\tau = \boxed{(1,2)(3,5,4,7)}$ and
(84b) $\sigma \circ \tau = (1,3,5,6)(1,2)(3,5,4,7)(1,3,5,6) = \boxed{(1,2,3,6)(4,7,5)}$.
(84c) $\boxed{\sigma = (1,3)(3,5)(5,6)}$ and $\boxed{\tau = (1,2)(3,5)(5,4)(4,7)}$

(85) List all of the elements of S_4. Use cycle notation.

Answer: The elements of S_4 are:

$$(1),\quad (1,2),\quad (1,3),\quad (1,4),\quad (2,3),\quad (2,4),\quad (3,4),\quad (1,2,3),\quad (1,3,2),$$
$$(1,2,4),\quad (1,4,2),\quad (1,3,4),\quad (1,4,3),\quad (2,3,4),\quad (2,4,3),\quad (1,2,3,4),$$
$$(1,2,4,3),\quad (1,3,2,4),\quad (1,3,4,2),\quad (1,4,2,3),\quad (1,4,3,2),\quad (1,2)(3,4),$$
$$(1,3)(2,4),\quad (1,4)(2,3)$$

(86) Find the number of cycles of each possible length in S_5. Find all possible orders of elements in S_5. (Try to do this problem without listing all of the elements of S_5.)

Answer: The group S_5 has $5! = 120$ elements. Each element of S_5 is a product of disjoint cycles. In the following discussion a,b,c,d,e are the distinct numbers $1,2,3,4,5$. Each element of S_5 has the form id or (a,b) with $a < b$, or (a,b,c) with $a < b$ and $a < c$, or (a,b,c,d) with $a < b$ and $a < c$ and $a < d$, or (a,b,c,d,e) with $a < b$ and $a < c$ and $a < d$ and $a < e$, or $(a,b)(c,d)$ with $a < b$ and $a < c < d$, or $(a,b)(c,d,e)$ with $a < b$ and $a < c$

and $c < d$ and $c < e$. Now we count the number of elements of each shape. At the same time we record the order of each element of a given shape.

cycle structure	number	order
id	1	1
(a,b)	$\binom{5}{2} = 10$	2
(a,b,c)	$2\binom{5}{3} = 20$	3
(a,b,c,d)	$3!\binom{5}{4} = 30$	4
(a,b,c,d,e)	$4!$	5
$(a,b)(c,d)$	$5(3) = 15$	2
$(a,b)(c,d,e)$	$2\binom{5}{2} = 20$	6
total	120	

There are $\binom{5}{2}$ ways to choose 2 numbers from $\{1,2,3,4,5\}$. Once you pick a two element subset of $\{1,2,3,4,5\}$, this subset corresponds to one two-cycle.

There are $\binom{5}{3}$ ways to choose 3 numbers from $\{1,2,3,4,5\}$. Once you pick a three element subset of $\{1,2,3,4,5\}$, this subset corresponds to two three-cycles.

There are $4! = 24$ 5-cycles in S_5. Put the smallest number (i.e., 1) first. Each order for $2,3,4,5$ gives rise to a new element of S_5.

There $\binom{5}{4} = 5$ ways to pick a four element subset of $\{1,2,3,4,5\}$. Once you pick a four element subset of $\{1,2,3,4,5\}$, this subset corresponds to $3! = 6$ four-cycles. (Put the smallest number first. Each of arrangements of the remaining three elements gives a new element of S_5.)

There are 5 ways to pick a four element subset of $\{1,2,3,4,5\}$. Once you select the subset $\{a,b,c,d\}$, this subset gives rise to 3 permuations of the form $(i,j)(k,\ell)$; namely $(a,b)(c,d)$, $(a,c)(b,d)$, and $(a,d)(b,c)$.

There are $\binom{5}{2} = 10$ ways to separate $\{1,2,3,4,5\}$ into two subsets so that one subset has two elements and the other subset has 3 elements. The subset with two elements gives rise to one two-cycle; the subset with three elements gives rise to two three cycles.

(87) Let S be a set and let a be an element of S. Prove that

$$\{\sigma \in \mathrm{Sym}(S) \mid \sigma(a) = a\}$$

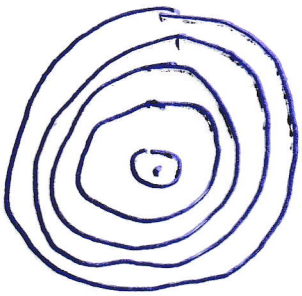
is a subgroup of $\mathrm{Sym}(S)$. Recall that $\mathrm{Sym}(S)$ is the group of permutations of S.

Answer: Let $H = \{\sigma \in \mathrm{Sym}(S) \mid \sigma(a) = a\}$. We show that H is closed. If σ and τ are in H, then σ and τ are in $\mathrm{Sym}(S)$, $\sigma(a) = a$, and $\tau(a) = a$. The operation $\circ$ makes $\mathrm{Sym}(S)$ a group. Groups are closed; hence $\sigma \circ \tau \in \mathrm{Sym}(S)$. Also, $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$ because σ and τ are both in H. We conclude that $\sigma \circ \tau$ is in H.

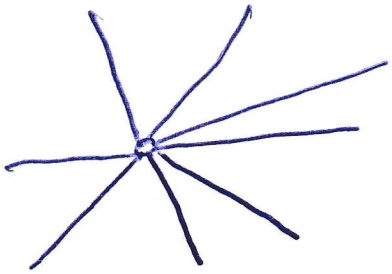
Keep the element σ of H. We know that $\mathrm{Sym}(S)$ is a group; so σ has an inverse σ^{-1} in $\mathrm{Sym}(S)$. We must show that σ^{-1} is in H. The function σ^{-1} undoes σ; that is, if $\sigma(x) = y$, then $\sigma^{-1}(y) = x$ for all x and y in S. In fact, $\sigma(a) = a$; hence $\sigma^{-1}(a) = a$ and σ^{-1} is in H.

Here is a solution to problems 3.11 and 3.12 from the class notes.

3.11 Each left coset of U in $(\mathbb{C}^\times, \times)$ has the form rU for some positive real number R. These cosets partition the complex plane (without zero) into concentric circles



3.12 Each left coset of $(\mathbb{R}^{pos}, \times)$ in $(\mathbb{C}^\times, \times)$ has the form $e^{i\theta}\mathbb{R}^{pos}$ for some real θ with $0 \leq \theta < 2\pi$. These cosets partition the complex plane (without 0) into rays emanating from 0



Here is a solution to problem 5.7 from the Class notes. We are asked to prove that S_n is isomorphic to a subgroup of $\mathrm{GL}_n(\boldsymbol{k})$ for each field $\boldsymbol{k}$ and each positive integer n. If σ is an element S_n, then let P_σ be the identity matrix with columns permuted according to σ; that is, put the $\sigma(1)$ column of the identity matrix first, the $\sigma(2)$ column of the identity matrix second, ..., and the $\sigma(n)$ column of the identity matrix last. For example, if $n = 3$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

then

$$P_\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad P_\tau = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Observe that

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_{\tau\circ\sigma} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \text{and}$$

$$P_\tau P_\sigma = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

It is clear that $\phi : S_n \to \mathrm{GL}_n(\boldsymbol{k})$, given by $\phi(\sigma) = P_\sigma$ is a well-defined injective function. "The usual manipulations" show that ϕ is a group homomorphism.

Maybe I will sketch "The usual manipulations" in case you don't have some of them from your linear algebra class. In this discussion we have three vector spaces U, V, and W. For each vector space we have a basis:

$$\begin{aligned} &\mathscr{B}, \text{ which is } u_1, \ldots, u_p, \text{ for } U, \\ &\mathscr{C}, \text{ which is } v_1, \ldots, v_q, \text{ for } V, \text{ and} \\ &\mathscr{D}, \text{ which is } w_1, \ldots, w_r, \text{ for } W. \end{aligned}$$

We also have two linear transformations: $S : U \to V$ and $T : V \to W$. If $u \in U$, then $[u]_{\mathscr{B}}$ represents the column vector of coefficients of u with respect to the basis $\mathscr{B}$ of U, that is

$$[u]_{\mathscr{B}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_p \end{bmatrix},$$

where $u = \sum_{i=1}^{p} \alpha_i u_j$. The coefficient vectors $[v]_{\mathscr{C}}$ and $[w]_{\mathscr{D}}$, for $v \in V$ and $w \in W$ are defined in a similar manner. The matrix for S with respect to the bases $\mathscr{C}$ and $\mathscr{B}$ is defined to be the $p \times q$ matrix $[S]_{\mathscr{C},\mathscr{B}}$ whose j-th column is $[u_j]_{\mathscr{B}}$. One easily checks that

$$[S]_{\mathscr{C},\mathscr{B}}[u]_{\mathscr{B}} = [S(u)]_{\mathscr{C}}$$

for all $u \in U$. One defines $[T]_{\mathscr{D},\mathscr{C}}$ in a similar manner. One checks that

$$[T]_{\mathscr{D},\mathscr{C}}[v]_{\mathscr{C}} = [T(v)]_{\mathscr{D}}$$

for all $v \in V$. At this point, one checks that

$$[T \circ S]_{\mathscr{D},\mathscr{B}} = [T]_{\mathscr{D},\mathscr{C}} \text{ times } [S]_{\mathscr{C},\mathscr{B}}$$

by verifying

$$[T \circ S]_{\mathscr{D},\mathscr{B}}[u]_{\mathscr{B}} = [T]_{\mathscr{D},\mathscr{C}}[S]_{\mathscr{C},\mathscr{B}}[u]_{\mathscr{B}}$$

for each $u \in U$.

This is Problem 6.13 from the class notes. Mimic Example 6.12 from the class notes in the situation where $T = \{x_1, x_2, x_3, x_4\}$. Which polynomial plays the role of Δ? Which elements of $\mathrm{Sym}(T)$ are in the kernel of ϕ. You might find it helpful to use cycle notation as described in section 7.A.

Observation 0.1. *Suppose that permutation σ in S_n is a product of a transpositions and also is a product of b transpositions. We claim that a and b are both even or a and b are both odd.*

Proof. It suffices to show that $(-1)^a = (-1)^b$. Consider the homomorphism

$$\phi : \mathrm{Sym}(\{x_1, \ldots, x_n\}) \to \mathrm{Sym}(\{\Delta, -\Delta\})$$

of Example 6.12, where

$$\Delta = \prod_{i<j} (x_j - x_i).$$

Claim 0.2. *If (k,ℓ) in S_n, then $(k,\ell)\Delta = -\Delta$.*

Proof of claim. It does no harm to assume that $k < \ell$. Observe that

$$\Delta = \Big(\prod_{\substack{i<j \\ \{i,j\}\cap\{k,\ell\}=\emptyset}} (x_j - x_i) \Big) \Big(\prod_{i<k} (x_k - x_i)(x_\ell - x_i) \Big) \Big(\prod_{k<i<\ell} (x_i - x_k)(x_\ell - x_i) \Big) \Big(\prod_{\ell<i} (x_i - x_\ell)(x_i - x_k) \Big) (x_\ell - x_k).$$

$$(k,\ell)(\Delta) = \Big(\prod_{\substack{i<j \\ \{i,j\}\cap\{k,\ell\}=\emptyset}} (x_j - x_i) \Big) \Big(\prod_{i<k} (x_\ell - x_i)(x_k - x_i) \Big) \Big(\prod_{k<i<\ell} (x_i - x_\ell)(x_k - x_i) \Big) \Big(\prod_{\ell<i} (x_i - x_k)(x_i - x_\ell) \Big) (x_\ell - x_k).$$

The four factors inside $\Big(\quad \Big)$ remain unchanged. The factor $(x_\ell - x_k)$ has changed to $(x_k - x_\ell) = -(x_\ell - x_k)$. The claim is established. □

The observation follows readily, because

$$\sigma(\Delta) = (-1)^a \Delta \quad \text{and} \quad \sigma(\Delta) = (-1)^b \Delta.$$

The polynomial Δ in $\mathbb{Z}[x_1, \ldots, x_n]$ is not identically zero; hence $(-1)^a = (-1)^b$, as desired. □

This is problem 6.18 from the class notes:

The groups $\frac{\mathbb{Z}}{\langle 8 \rangle}$, $\frac{\mathbb{Z}}{\langle 4 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle}$, and $\frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle}$ are Abelian. The groups D_4 and Q_8 are not Abelian. If two groups are isomorphic then they are both Abelian or neither one is Abelian.

The group $\frac{\mathbb{Z}}{\langle 8\rangle}$ has an element of order 8; neither of the groups $\frac{\mathbb{Z}}{\langle 4\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ nor $\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ has an element of order 8.

The group $\frac{\mathbb{Z}}{\langle 4\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ has an element of order four, but $\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ does not have an element of order four.

The group D_4 has many elements of order two. The group Q_8 has only one element of order two.

This is problem 7.10 from the class notes. How do we know that A_4 does not have any subgroups of order six? (I first told you this as an example of why the converse of Lagrange's Theorem is not true. This is the smallest such example.)

The group A_4 has twelve elements; namely

$$(1),(123),(132),(124),(142),(134),(143),(234),(243),(12)(34),(13)(24),$$
$$(14)(23).$$

We argue by contradiction. Suppose that H is a subgroup of A_4 of order 6, then H has index 2 in A_4; consequently, H is a normal subgroup of A_4. The subgroup H must contain a three cycle (because all of the elements of A_4, except 4 are three cycles.) So, $\sigma=(i,j,k)\in H$ for three distinct integers i,j,k between 1 and 4 and $\sigma^{-1}=(ikj)\in H$. Let ℓ be the fourth integer between 1 and 4. Observe that

$$(i\ell j)(ijk)(ij\ell)=(ik\ell)\in H$$

and

$$(ik\ell)^{-1}=(i\ell k)\in H.$$

Similarly,

$$(i\ell j)(i\ell k)(ij\ell)=(jk\ell)\in H$$

and

$$(jk\ell)^{-1}=(j\ell k)\in H.$$

At this point H contains at least 7 elements. We have reached a contradiction; because H contains exactly six elements.

We conclude that H does not exist.